SPECIFICATION

Please amend the specification in accordance with 37 C.F.R. § 1.121(b)(1) as follows:

On page 30, line 18, please delete the paragraph that begins "Refer now to FIG. 9 ..." and replace it with the following paragraph, with markings as required by 37 C.F.R. § 1.121(b)(1)(ii):

Refer now to FIG. 9 for a discussion of the steps of the preferred packet classifier, flow collector, and alert or alarm manager threads. As previously discussed in reference to FIG. 5, the preferred flow-based intrusion detection engine 155 comprises three operational threads or processes that execute within a system or appliance that implements an embodiment of the invention. The packet classifier thread 510 (FIG. 9A) classifies packets into their associated flow and updates the flow records. The flow collector thread (FIG. 9B) 520 determines a termination of a flow, performs a logic tree analysis to classify the flow, and assigns a corresponding CI value in response to detection of activity warranting an increase in the CI. Finally, the alert or alarm manager thread 530 (FIG. 9C) generates reports and alarm signals if an alarm threshold is exceeded.

As required by 37 C.F.R. § 1.121(b)(1)(iii), here is the full text of the paragraph without underlining:

Refer now to FIG. 9 for a discussion of the steps of the preferred packet classifier, flow collector, and alert or alarm manager threads. As previously discussed in reference to FIG. 5, the preferred flow-based intrusion detection engine 155 comprises three operational threads or processes that execute within a system or appliance that implements an embodiment of the invention. The packet classifier thread 510 (FIG. 9A) classifies packets into their associated flow and updates the flow records. The flow collector thread (FIG. 9B) 520 determines a termination of a flow, performs a logic tree analysis to classify the flow, and assigns a corresponding CI value in response to detection of activity warranting an increase in the CI. Finally, the alert or alarm manager thread 530 (FIG. 9C) generates reports and alarm signals if an alarm threshold is exceeded.

On page 30, line 28, please delete the paragraph that begins "In FIG. 9A ... " with the following paragraph (to correct "flow classifier 510" to --packet classifier 510--), with markings as required by 37 C.F.R. § 1.121(b)(1)(ii):

In FIG. 9A, the packet ~~flow~~ classifier thread 510 begins with step 912. In step 912, the thread 510 determines if a new packet is available. If a new packet is not available, the no branch of step 912 is followed to step 912, in which the thread 510 awaits a new packet. If a new packet is available, the yes branch of step 912 is

followed to step 914, in which the thread determines if the packet belongs to a new flow.

As required by 37 C.F.R. § 1.121(b)(1)(iii), here is the full text of the paragraph without underlining:

In FIG. 9A, the packet classifier thread 510 begins with step 912. In step 912, the thread 510 determines if a new packet is available. If a new packet is not available, the no branch of step 912 is followed to step 912, in which the thread 510 awaits a new packet. If a new packet is available, the yes branch of step 912 is followed to step 914, in which the thread determines if the packet belongs to a new flow.